## CLAIMS

**We claim**:

1. A method enabling a network-addressable device to detect use of its identity by a spoofer, comprising the acts of:

receiving a message by the network-addressable device;

detecting a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of activity of a spoofing vandal using an identity of the network-addressable device; and

generating a spoofing alert responsive to the act of detecting the communication protocol violation.

2. A method enabling a network-addressable device to detect use of its identity by a spoofer, comprising the acts of:

receiving a message by the network-addressable device;

detecting a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of activity of a spoofing vandal using the identity of the network-addressable device in an attack on a target;

recording attributes of the message;

advancing the value of a counter associated with the target;

comparing the value of the counter with a predetermined threshold; and

generating a spoofing alert when the value of the counter exceeds the threshold.

3. The method of claim 2, further comprising the act of sending the spoofing alert to a network administrator.

4. The method of claim 3, wherein the network administrator is associated with the network-addressable device.

5. The method of claim 3, wherein the network administrator is associated with the target.

6. The method of claim 2, further comprising the act of blocking the message.

7. The method of claim 2, wherein the act of recording attributes of the message includes the act of writing a record to a spoofing logbook database.

8. The method of claim 2, wherein the act of recording attributes of the message includes the act of writing the message to a spoofing logbook database.

9. The method of claim 2, wherein the identity of the network-addressable device is a TCP/IP source address of the network-addressable device.

10. The method of claim 2, wherein the protocol violation includes reception by the network-addressable device of an unsolicited response message sent by the target.

11. The method of claim 2, wherein the protocol violation includes the reception by the network-addressable device of an ICMP reply sent by the target when an ICMP PING has not been sent to the target by the network-addressable device.

12. The method of claim 2, wherein the protocol violation includes reception by the network-addressable device of a SYN/ACK message when a SYN message has not been sent to the target by the network-addressable device.